

Please type a plus sign (+) inside this box → ☐

PTO/SB/05 (4/98)

Approved for use through 09/30/2000. OMB 0651-0032

Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No. 500.38618X00

First Inventor or Application Identifier Atsushi MAEDA, ET AL

Title A METHOD FOR MANAGING PUBLIC KEY

Express Mail Label No.

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☒ Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)
2. ☒ Specification [Total Pages 24]
(preferred arrangement set forth below)
 - Descriptive title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
3. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets 6]
4. Oath or Declaration [Total Pages]
 - a. ☐ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 15 completed)
 - i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13 IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28)

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

5. ☐ Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy (identical to computer copy)
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☐ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. §3.73(b) Statement of Attorney
(when there is an assignee)
9. ☐ English Translation Document (if applicable)
10. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
13. ☐ Small Entity Statement(s) ☐ Statement filed in prior application
(PTO/SB-09-12) Status still proper and desired
14. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☒ Other: See 1 in Addendum

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: /

Prior application information: Examiner

Group / Art Unit:

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label

020457

or ☐ Correspondence address below

(Insert Customer No. or Attach bar code label here)

Name			
Address			
City	State	Zip Code	
Country	Telephone	Fax	

Name (Print/Type) Carl J. Brundridge

Registration No. (Attorney/Agent) 29,621

Signature

Date 06/02/2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

E-5272-01EK

A METHOD FOR MANAGING PUBLIC KEY

002090.85E58560

BACKGROUND OF THE INVENTION

本発明は、公開鍵の管理方法に係り、特に、ネットワークにおけるセキュリティ技術に使用される公開鍵暗号システムに使用して好適な公開鍵の管理方法に関する。

インターネットを使用してセキュリティ通信を実現する方法として、例えば、IP (Internet Protocol) レイヤのセキュリティプロトコルである IPSEC (IP Security) がある。IPSEC に関する技術文献として、例えば、IETF (Internet Engineering Task Force) 発行の [RFC1825] “Security Architecture for the Internet Protocol.” (R. Atkinson 著) 等が知られている。

IPSEC に付随する鍵管理プロトコルは、公開鍵暗号システムを利用するものである。鍵管理プロトコルに関する従来技術として、例えば IETF 発行の “Simple Key-Management For Internet Protocol.” (著者: Ashar Aziz, Tom Markson, Hemma Prafullchandra) 等に記載された SKIP と呼ばれる技術が知られている。以下、この鍵管理プロトコルについて説明する。

いま、ネットワーク内にセキュリティ通信を行う 2 つのホスト A、B があり、これらのホスト A、B は、IPSEC に基づいた共通鍵暗号システムによって暗号通信を行うものとし、ホスト A は、ホスト B の公開鍵を、ホスト B は、ホスト A の公開鍵を知っているものとする。

ホスト A と B とは、通信を行うに際して、既知のアルゴリズムを用いてそれぞれ自らの秘密鍵と相手の公開鍵とを組み合わせることで共通鍵を暗号化するための鍵 K (A)、K (B) を生成する。ここで、例えば、ホスト A がホスト B にデータを送信するとき、ホスト A は、共通鍵 T を生成し、それを用いてデータを暗号化し、鍵 K (A) を用いて共通鍵 T を暗号化する。ホスト A は、暗号化された共通鍵 T の情報を含む新たなヘッ

ダをIPヘッダの後に挿入する。受信側のホストBは、自らが持つ秘密鍵によって、パケットの中にある暗号化された共通鍵Tを解読し、解読した共通鍵Tによって暗号化されたパケットのデータを解読する。そして、このようなホストA、B間のセキュリティ通信において、データを暗号化するための共通鍵は、定期的に更新される。

前述したようなIPSECに付随する従来技術による鍵管理プロトコルは、セキュリティ通信を行う2つのホストが通信開始前に互いに相手の公開鍵を知っていることが前提とされている。

前述した従来技術による方法は、セキュリティ通信を行おうとする2つのホストが、通信開始前にお互いの公開鍵を自動的かつ安全に交換する方法がなく、その結果、手渡しによる公開鍵の交換等の方法に頼ることになり、公開鍵の管理が複雑になっているという問題点を有している。また、この結果、前述の従来技術は、ネットワークの規模が大きい場合、ネットワークの管理者に対する負担が大きくなるという問題点を生じさせている。

さらに、前述の従来技術は、ネットワーク上の認証を伴わない公開鍵の配布を行った場合、不正なホストがセキュリティ通信の相手になりすますことを防ぐことができないという問題点をも有している。

SUMMARY OF THE INVENTION

本発明の目的は、前述した従来技術の問題点を解決し、セキュリティ通信を行おうとする2つのホストが通信開始前にお互いの公開鍵を自動的かつ安全に交換することを可能にした公開鍵の管理技術を提供することにある。

本発明によれば前記目的は、階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるDNSサーバと、ネットワークに収容されるホストとを備え、前記DNSサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理システムにおいて、前記DNSサーバが、公開鍵を管理する手段と、前記ネットワ

また、前記目的は、前記DNSサーバが、第1のホストから第2のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のDNSサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することにより達成される。

さらに、前記目的は、前記ホストが、前記DNSサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記DNSサーバに問い合わせることにより達成される。

本発明の目的は、前述の手段を持つ構成以外に、さらに、次に示すような手段を備えることによって達成することができる。

すなわち、前記目的は、ネットワークの構成に変更が生じた場合、構成の変化に
関係する一部のDNSサーバが、ホストの公開鍵とドメイン名のと対応を格納してい
るデータベースを更新し、前記以外のDNSサーバがデータベースの更新を行わない
ようにすることにより達成される。

また、前記目的は、前記公開鍵管理手段とデータベースとを備えたDNSサーバと、前記公開鍵を問い合わせる手段を備えたホストとに電子署名を処理する手段を設け、公開鍵問い合わせ及び応答のために出力するパケットに電子署名を付け、電子署名の付いた入力パケットについて、その電子署名を確認し、改竄されている入力パケットを廃棄することにより、パケットの内容が改竄されるのを防止するようにすることにより達成される。

また、前記目的は、前記DNSサーバに対してホストが送信する公開鍵問い合わせパケットの中にホストが信用するDNSサーバのドメイン名の情報を含め、公開鍵の情報を応答する前に、前記DNSサーバの公開鍵管理手段に、公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに対して電子署名を要求させ、電子署名の要求を受けたDNSサーバの公開鍵管理手段に、公開鍵応答パケットに電子署名を付けさせ、その電子署名により公開鍵応答パケットに含まれる公開鍵の情報が信用できるか否かを前記ホストの電子署名を処理する手段に判定させ、これにより、不正なホストが自分の公開鍵とアドレスとを公開鍵問い合わせパケットの中にある問い合わせドメイン名に対応しているように見せかけることを防止するようにしたことにより達成される。

また、前記目的は、電子署名の要求を受けたDNSサーバが公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバと異なるとき該DNSサーバの公開鍵管理手段は、ドメイン名の階層構造に沿って、上位のDNSサーバに公開鍵応答パケットに対する電子署名を要求し、最終的には公開鍵問い合わせパケットの中で示されるホストが信用するDNSサーバに公開鍵応答パケットに電子署名を付けさせることにより達成される。

また、前記目的は、前記ホストの公開鍵問い合わせ手段に、問い合わせるドメイン名に従って信用するDNSサーバを選択させ、公開鍵問い合わせパケットの中に該DNSサーバのドメイン名の情報を含め、公開鍵応答パケットに電子署名を付ける処理を行うDNSサーバの数を減らすことにより公開鍵の取得を効率的なものとする
ことにより達成される。

また、前記目的は、電子署名付きの公開鍵の応答を受けたDNSサーバの公開鍵

BRIEF DESCRIPTION OF THE DRAWINGS

図 1 は本発明の一実施形態における KMS (Key Management Server) の構成を示すブロック図である。

図 2 は上記実施形態における DNS クライアントの機能を持つホストの構成を示すブロック図である。

図 3 は上記実施形態における公開鍵とドメイン名との対応を説明するテーブルの構成を示す図である。

図 4 は DNS サーバが公開鍵の問い合わせを受けたときに公開鍵を応答する手順を説明するフローチャートである。

図 5 は DNS サーバが電子署名の要求を受けたときに公開鍵応答パケットに電子署名を付与する手順を説明するフローチャートである。

図 6 は DNS クライアントの機能を持つホストが通信相手の公開鍵を取得する手順を説明するフローチャートである。

図 7 は本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の実施形態を示すブロック図である。

図 8 はホストが通信相手の公開鍵の取得ために行う手順の中で、ホスト・KMS 間及び KMS・KMS 間でやり取りするパケットの種類とそれらに付与される電子署名を説明する図である。

図 9 は DNS パケットのフォーマットの構成を説明する図である。

図 10 は DNS パケットに含まれる資源レコードのフォーマットの構成を説明する図である。

DESCRIPTION OF THE EMOIDIMENTS

以下、本発明を用いた公開鍵管理システムの実施形態を図面を参照して詳細に説明する。

S パケットに含まれる資源レコードのフォーマットの構成とを説明する。

DNSパケットは、図9に示すように、DNSヘッダ91、問い合わせ部92、回答部93、権限付きネームサーバの名前を表す権威部94、複数の資源レコードを含む付加情報部95から成る。また、図10に示すように、DNSパケットに含まれる資源レコードの1つであるTXTレコードは、名前フィールド101、TYPEフィールド102、CLASSフィールド103、この資源レコードが捨てられずにキャッシュされている時間間隔を示すTTLフィールド104、データ長フィールド105、データフィールド106からなる。

複数の資源レコードとしては、TYPEにより識別される複数のものがあり、本発明の実施形態においては、複数のDNS資源レコードの内TXTレコードと呼ばれるTYPE＝16の資源レコードに、公開鍵問い合わせ情報及び公開鍵応答情報を入れることとする。また、本発明の実施形態は、公開鍵問い合わせ情報及び公開鍵応答情報を入れる資源レコードのデータフィールド106の先頭に公開鍵問い合わせ／応答、電子署名要求、または、通常のTXTレコードの区別がつくような識別子1061のフィールドを設けている。

なお、TXTレコードについては、前掲のDNSに関する文献の中に説明がある。また、資源レコードとして、前述したTXTレコードの他に、アドレスとドメイン名との対応を示すAレコード（TYPE＝1）、メール・エクスチェンジャのドメイン名を示すMXレコード（TYPE＝15）等がある。

次に、図1を参照して、本発明の実施形態によるサーバであるKMSの構成を説明する。図1において、各ブロックを結ぶ実線はパケットの受け渡しを行う関係を示し、破線はデータの参照を行うことを示す。

KMS10は、ネットワーク制御部11と、IP処理部12と、TCP/UDP処理部13と、拡張DNS処理部14と、ドメイン名・IPアドレステーブル15と、ドメイン名・公開鍵・電子署名テーブル16と、初期保持データ17とを備えて構成され、ネットワーク制御部11を介してネットワーク101に接続されている。また、

拡張DNS処理部14は、DNSパケット振り分け部141と、DNS処理部142と、公開鍵問い合わせ／応答処理部143と、電子署名処理部144とを備えて構成されている。

前述において、ネットワーク制御部11は、KMS10とIPネットワーク101とを接続している。IP処理部12は、ネットワーク制御部11の上位にあって、IP (Internet Protocol) によってやり取りされるパケットの送受信処理を行う。TCP/UDP処理部13は、IP処理部12の上位にあって、TCP/UDP (Transmission Control Protocol/User Datagram Protocol) によってやり取りされるパケットの送受信処理を行う。ここで、特に、TCP/UDP処理部13は、DNSに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張DNS処理部14に送る。逆に、拡張DNS処理部14は、自ら生成したパケットを送信するとき、その送信すべきパケットをTCP/UDP処理部13に送る。

拡張DNS処理部14におけるDNSパケット振り分け部141は、TCP/UDP処理部13からDNSパケットを受け取り、図10に示す識別子1061を見てDNS処理部142、公開鍵問い合わせ／応答処理部143、電子署名処理部144の内のどれかにDNSパケットを振り分ける。DNS処理部142は、TCP/UDP処理部13からの従来のDNSパケットを受け取り、ドメイン名とIPアドレスとが対応づけて格納されているデータベースであるドメイン名・IPアドレステーブル15の検索またはエントリの追加を行う。公開鍵問い合わせ／応答処理部143は、他のKMSからの公開鍵の問い合わせを拡張DNSパケットの形でTCP/UDP処理部13から受け取ったとき、問い合わせのあったドメイン名の公開鍵を取得するためにドメイン名と公開鍵とが対応づけて格納されたドメイン名・公開鍵・電子署名テーブル16を検索する。

ドメイン名・公開鍵・電子署名テーブル16は、図3に示すように、ドメイン名31、公開鍵32、ホストが信用するKMSが付けた電子署名33、電子署名を付けたKMSのKMS名34、エントリの生成時点を示すタイムスタンプ35の5つの項

ている。TCP/UDP処理部23は、DNSに割り当てられたソケット番号を持つパケットを受信したとき、そのパケットを拡張DNSクライアント24に送る。逆に、拡張DNSクライアント24は、自ら生成したパケットを送信するとき、そのパケットをTCP/UDP処理部23に送る。

拡張DNSクライアント24内のDNSパケット振り分け部241は、TCP/UDP処理部23からDNSパケットを受け取り、DNSヘッダの中身を見てドメイン名リゾルバ242、公開鍵問い合わせ処理部243のいずれかに処理を振り分ける。ドメイン名リゾルバ242は、従来のDNSクライアントと同様に、ドメイン名に対応するIPアドレスを解決する処理を行う。そして、ドメイン名に対応するIPアドレスを問い合わせる際、ドメイン名リゾルバ242は、TCP/UDP処理部23を通して問い合わせパケットを送信する。ドメイン名リゾルバ242は、問い合わせに対する応答もTCP/UDP処理部23を通して受信する。

本発明により新たに付加したモジュールである公開鍵問い合わせ処理部243は、ドメイン名に対応する公開鍵を解決する処理を行う。公開鍵問い合わせ処理部243は、新規に得た公開鍵の情報をドメイン名・公開鍵・電子署名テーブル25に保存し、次回に公開鍵を問い合わせに行く前に参照する。電子署名確認部244は、公開鍵問い合わせ処理部243が受け取った公開鍵の情報について、初期保持データ26内の信用するKMSのドメイン名・公開鍵263を参照して、公開鍵の情報に付いている電子署名が信用するKMSのものか否かを判定し、公開鍵の情報が信用できるか否かを確認する。

公開鍵問い合わせ処理部243は、信用するKMSのドメイン名・公開鍵263が複数ある場合に、公開鍵を問い合わせるドメイン名に応じて信用するKMSのドメイン名・公開鍵263の中から最適な信用するKMSを選択する。ホスト20は、初期保持データ26内に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを持ち、公開鍵問い合わせ処理部243は、公開鍵を問い合わせに行く際に自分のドメイン名・公開鍵261と上位のKMSのドメイン名262とを参照する。

セキュリティ通信処理部27は、公開鍵問い合わせ処理部243が取得した通信相手の公開鍵に基づいて、従来の方法に従ってセキュリティ通信を行う。

次に、図4に示すフロー、及び、ホスト・KMS間及びKMS・KMS間でやり取りするパケットの種類とそれらに付与される電子署名を示す図8を参照して、本発明を階層的なドメイン名の構造を持つネットワークに適用した場合の図7に示すネットワークにおいて、ホストが通信相手の公開鍵の取得ために行う手順について説明する。

図7において、KMS0(73)、KMS1(72)、KMS2(76)、KMS00(74)は、図1により説明した構成を持つKMSであり、また、ホストA71、B75は、図2により説明した構成の拡張したDNSクライアントの機能を持つホストである。そして、KMS00(74)は、ドメイン名xxを持つネットワーク701に接続され、KMS0(73)は、ドメイン名a.xxを持つネットワーク702に接続されている。また、ホストA71とKMS1(72)とは、ドメイン名b.a.xxを持つネットワーク703に接続され、ホストB75とKMS2(76)とは、ドメイン名c.a.xxを持つネットワーク704に接続されている。

ドメイン名は、階層構造を成しており、各KMSは、従来のDNSサーバの役割をも果たしている。また、図8に示す例は、ホストB75の公開鍵の情報をKMS2(76)のみが持っている場合の各KMSの動作を示しており、また、図8に示す各矢印は、ホストA71がホストB75の公開鍵を取得する際に、ホストとKMSとの間やKMSとKMSとの間でやり取りするパケットやパケットに付加する電子署名の形態を示している。パケットの種類は、公開鍵問い合わせ、電子署名要求、公開鍵応答の3通りあり、電子署名の具体的な内容は、図8の枠内の記号を用いて表しているように、次のように定義されているものとする。

S(K, [a, b, c]) : 鍵Kによりメッセージ[a, b, c]に電子署名を付与したもの

D(X) : Xのドメイン名

S (X) : Xの公開鍵

T (X) : Xの秘密鍵

I P (X) : XのI Pアドレス

KMS (X) : Xが電子署名を要求するKMS

以下、ホストA 7 1が電子署名を要求するKMSがKMS 0 0 (7 4)であるとして図4に示すフローを説明する。

(1) まず、ホストAは、ホストB 7 5の公開鍵を問い合わせるパケットをKMS 1 (7 2)に送信する。この公開鍵を問い合わせるパケットは、図8に矢印8 1により示しているように、

S (T (A) , [D (B) , KMS (A) , I P (A) , D (A)])

であり、これは、前述の定義から理解できるように、ホストBのドメイン名、ホストAが電子署名を要求するKMS、ホストAのI Pアドレス、ホストAのドメイン名よりなるメッセージに、ホストAの秘密鍵により電子署名を行ったものである。KMS 1 (7 2)がホストA 7 1からホストB 7 5の公開鍵を問い合わせるパケットを受けるとき、図1に示す電子署名処理部1 4 4は、パケットに付いている電子署名を見る。電子署名処理部1 4 4は、ドメイン名・公開鍵・電子署名テーブル1 6からホストA 7 1の公開鍵を取り出し、パケットの内容が改竄されていないか否かをその公開鍵を使って判定する(ステップ4 1)。

(2) KMS 1 (7 2)は、ステップ4 1の判定で、問い合わせパケットが改竄されていた場合、そのパケットを廃棄して処理を終了し、問い合わせパケットが改竄されていない場合、図1に示す公開鍵問い合わせ/応答処理部1 4 3を動作させ、問い合わせのドメイン名についてドメイン名・公開鍵・電子署名テーブル1 6にエントリがあるか否かを検索する。ここで、タイムスタンプも参照し、一定時間以上過ぎている場合、無効なエントリと見做す(ステップ4 3、4 2)。

(3) ステップ4 2の判定で、ドメイン名・公開鍵・電子署名テーブル1 6にエントリがなかったとき、図7に示すKMS 1 (7 2)の公開鍵問い合わせ/応答処理部1 4

3は、問い合わせのあったホストのドメイン名と自分のドメイン名とについてそれぞれが属するネットワークの名前が一致するか否か判定する。例えば、図7において、問い合わせのホストがB75である場合、B75の属するネットワークのドメイン名c. a. x xとKMS1(72)の属するネットワークのドメイン名b. a. x xは一致しない(ステップ44)。

(4) ステップ44の判定においてネットワークの名前が一致したとき、図7のKMS1(72)は、ホストA71に対してホストBに対する公開鍵が未解決であることを通知する(ステップ45)。

(5) ステップ44の判定においてネットワークの名前が一致しなかったとき、KMS1(72)は、図1にける初期保持データ17内の上位のKMSのドメイン名172を参照して問い合わせ先を調べ、KMS0(73)にホストB75の公開鍵を問い合わせる。この場合の問い合わせパケットは、図8に矢印82により示すように、

S(T(KMS1), [D(B), KMS(A), IP(KMS1), D(KMS1)]))であり、ホストB75のドメイン名、ホストA71が電子署名を要求するKMSのドメイン名、KMS1(72)のIPアドレス及びKMS1(72)のドメイン名をメッセージとし、KMS1(72)の秘密鍵を電子署名の鍵とする電子署名を付加して構成される。このように、電子署名を付加することによって問い合わせパケットの不正な改竄を防止することができる(ステップ46)。

(6) 次に、KMS1(72)は、自KMSに公開鍵を問い合わせた者がホストかKMSかを公開鍵問い合わせパケットの始点IPアドレスから判定し、公開鍵を問い合わせたのがKMSである場合、処理を終了する(ステップ461)。

(7) ステップ461で、自KMSに公開鍵を問い合わせた者がホストである場合、公開鍵問い合わせ/応答処理部143は、上位のKMSから公開鍵の応答があるまで一定時間待ち、一定時間内に公開鍵の応答がなく、電子署名付きの公開鍵を取得できなかった場合、処理を終了する(ステップ462、463)。

(8) 公開鍵問い合わせ/応答処理部143は、電子署名付きの公開鍵の応答が一定

時間内にあった場合、その公開鍵を図1に示すドメイン名・公開鍵・電子署名テーブル16にキャッシングする。このようにキャッシングを行うことにより、別のホストから同じドメイン名について公開鍵の問い合わせがあったときに、公開鍵問い合わせ／応答処理部143は、再度別のKMSに公開鍵の問い合わせに行かずに済み、公開鍵を解決する処理を効率的に行うことができる（ステップ464）。

(9) 次に、公開鍵問い合わせ／応答処理部143は、図8の矢印87に示すように自らの電子署名をつけた公開鍵応答パケットを公開鍵の問い合わせを受けたホストに返す。この電子署名付きの公開鍵応答パケットは、D(KMS1)、D(B)、S(B)、S(T(KMS00))、[D(B)、S(B)、D(KMS00)]をメッセージとし、秘密鍵T(KMS1)を署名の鍵とするものである（ステップ465）。

(10) ステップ42のデータベースの検索で、問い合わせのドメイン名について、ドメイン名・公開鍵・電子署名テーブル16にエントリがあった場合、図1に示す公開鍵問い合わせ／応答処理部143は、そのエントリに指定されたKMSの電子署名が付いているか否かを見る（ステップ47）。

(11) ステップ47のチェックで、指定されたKMSの電子署名がエントリに付いていた場合、公開鍵問い合わせ／応答処理部143は、そのエントリにある電子署名付きの公開鍵をホストA71に返す（ステップ48）。

(12) 一方、ステップ47で指定されたKMSの電子署名がエントリに付いていなかった場合、公開鍵問い合わせ／応答処理部143は、パケットに付いているホストA71が信用するKMSと図1の初期保持データの上位のKMSのドメイン名172を見て、図7に示すKMS0(73)に電子署名の要求を出す。図7に示すKMS2(76)がホストB75の公開鍵の情報を持っていて、KMS0(73)に電子署名の要求を出す場合、図8の矢印84に示すように、[D(B)、KMS(A)、IP(KMS1)、S(B)及びD(KMS2)]をメッセージとして、KMS2(76)の秘密鍵を鍵とする電子署名を付けて要求を行う（ステップ49）。

前述では、図7におけるKMS1(72)の動作について説明したが、他のKMS

0(73)、KMS2(76)も、前述したKMS1(72)の場合と同様な動作を行う。

次に、図5に示すフローと図7及び図8とを参照して、図1に示すKMSの各部の動作の中での電子署名の要求と応答とについて説明する。

(1) いま、図7に示すKMS0(73)が、KMS1(72)から電子署名の要求を受けたとする。この場合、KMS0(73)は、図1に示ような構成を持つ自装置内の電子署名処理部144を動作させ、パケットに付いている電子署名を見る。電子署名処理部144は、ドメイン名・公開鍵・電子署名テーブル16からKMS172の公開鍵を取り出し、パケットの内容が改竄されていないか否かを判定する(ステップ51)。

2) ステップ51の判定で、パケットの内容が改竄されていた場合、電子署名処理部144はパケットを廃棄し、KMS0(73)は処理を終了する(ステップ53)。

(3) ステップ51の判定で、パケットの内容が改竄されていなかった場合、電子署名処理部144は、パケットの内容を見て電子署名の要求先が自分自身か否かを判定する(ステップ52)。

(4) ステップ52の判定で、電子署名の要求先が自分自身でない場合、電子署名処理部144は、初期保持データの上位のKMSのドメイン名172を参照し、電子署名の要求を上位のKMSに対して出す。図7において、ホストA71が電子署名を要求するKMSがKMS00(74)である場合、図8の矢印85に示すように、KMS0(73)からKMS00(74)への電子署名要求パケットは、[D(B)、KMS(A)、IP(KMS1)、S(B)及びD(KMS0)]をメッセージとしKMS0(73)の秘密鍵を鍵とする電子署名を付けたものとなる(ステップ54)。

(5) 一方、ステップ52の判定で、電子署名の要求先が自分自身であった場合、電子署名処理部144は、要求されたパケットに対して自分の秘密鍵によって電子署名を付け、要求元のKMSに電子署名付きのパケットを返す。説明している例で、例えば、署名要求に対してKMS00(74)がKMS1(72)へ公開鍵を応答するものとする、その場合の応答パケットは、図8の矢印86に示すように、[D(B)、S(B)及びD(KMS00)]をメッセージとしKMS00(74)の秘密鍵を鍵とす

る電子署名を付けたものとなる（ステップ55）。

次に、図6に示すフローと図7及び図8とを参照して、図2に示す構成のホストの動作を説明する。

（1）図7において、ホストA71がホストB75の公開鍵を取得しようとするものとする。このとき、図2に示す構成を持つホストA71の公開鍵問い合わせ処理部243は、ドメイン名・公開鍵・電子署名テーブル25を検索しホストB75のエントリがあるか否かを調べる（ステップ61）。

（2）ステップ61で、ドメイン名・公開鍵・電子署名テーブル25にホストB75のエントリがなかったとき、公開鍵問い合わせ処理部243は、初期保持データ26の信用するKMSのドメイン名・公開鍵263を参照して信用するKMSを選択し、信用するKMSのドメイン名・公開鍵263が複数ある場合、問い合わせるドメイン名より上位にあつてそれに最も近いKMSを選択する（ステップ62）。

（3）次に、公開鍵問い合わせ処理部243は、初期保持データ26内の公開鍵を問い合わせに行くKMSのドメイン名262を参照して、そのKMSにホストB75の公開鍵を問い合わせる。この場合の公開鍵問い合わせパケットは、図8の矢印81に示すように、[D（B）、KMS（A）、IP（A）及びD（A）]をメッセージとし、ホストAの秘密鍵T（A）を鍵とする電子署名を付加したものとなる（ステップ63）。

（4）ホストA71は、ステップ63での問合せに対して、公開鍵応答パケットが返ってきたとき、図2の電子署名確認部244を動作させ、公開鍵応答パケットに付いている電子署名が要求したKMSのものであつて、かつパケットの内容が改竄されていないかを確認する（ステップ64）。

（5）一定時間以内に公開鍵応答パケットが返ってこないとき、あるいは、ステップ64で、公開鍵応答パケットに付いている電子署名が要求したKMSのものでないか、パケットの内容が改竄されていると判定された場合、ホストA71は、何もせずに処理を終了する。これにより、ネットワーク上にある不正なホストが自らの公開鍵とア

ビーして実現することができる。

09585358.060200

CLAIMS

1. 階層構造を持ち、各階層毎にドメイン名を持つネットワークと、そのドメイン名とアドレスとの対応を管理する前記各階層毎に設けられるDNSサーバと、ネットワークに収容されるホストとを備え、前記DNSサーバが、ネットワークに属するホストに対して他のホストが持つ公開鍵を配布する公開鍵管理方法において、前記DNSサーバは、公開鍵を管理する手段と、前記ネットワークに属するホストの公開鍵とドメイン名とを対応付けて格納したデータベースとを持ち、第1のホストからのドメイン名の情報による第2のホストの公開鍵の問い合わせを受けたとき、前記公開鍵管理手段が前記データベースを参照することにより、前記ドメイン名に対応する第2のホストの公開鍵の情報を前記第1のホストに応答することを特徴とする公開鍵管理方法。

2. 前記DNSサーバは、第1のホストから第2のホストの公開鍵の問い合わせを受けたとき、自サーバ内の前記データベースの中に問い合わせのドメイン名に対応するエントリがない場合、他の公開鍵管理手段とデータベースとを備えた他のDNSサーバに公開鍵の解決をドメイン名の階層に沿って再帰的に委託することを特徴とするクレーム1の公開鍵管理方法。

3. 前記ホストは、前記DNSサーバに他のホストの公開鍵を問い合わせる手段を備え、セキュリティ通信開始時、前記公開鍵問い合わせ手段に通信相手となるホストのドメイン名に対応する公開鍵を前記DNSサーバに問い合わせることを特徴とするクレーム1の公開鍵管理方法。

4. クレーム1の公開鍵管理方法を実現するための、DNSサーバに設けられる公開鍵を管理する手段の機能を実行するプログラムと、ネットワークに属するホスト

の公開鍵とドメイン名とを対応付けて格納するデータベースと、ホストからドメイン名の情報によって公開鍵の問い合わせを受けたとき該公開鍵管理手段が前記データベースを参照することによりドメイン名に対応する公開鍵をホストに応答する処理を実行するプログラムとを格納したことを特徴とする記憶媒体。

0058358-00000

ABSTRACT OF THE DISCLOSURE

階層構造のドメイン名の構成を持ち、そのドメイン名とアドレスとの対応を管理するDNSサーバが階層毎にあるネットワークにおいて、公開鍵を管理するモジュールとネットワークに属するホストの公開鍵とドメイン名との対応を示すデータベースを各DNSサーバに設ける。2つのホストがセキュリティ通信を開始するとき、一方のホストが前述の機能拡張したDNSから通信相手のホストの公開鍵を自動的に取得する。このとき、公開鍵問い合わせパケットの中にホストが信用するDNSサーバの名前を入れさせ、このホストが指定するDNSサーバが、公開鍵応答パケットに電子署名を付ける。ホストは、この電子署名により公開鍵応答パケットにある公開鍵が信用できるかどうかを判定することができ、不正なホストが通信相手になりすますのを防止する。

図 1

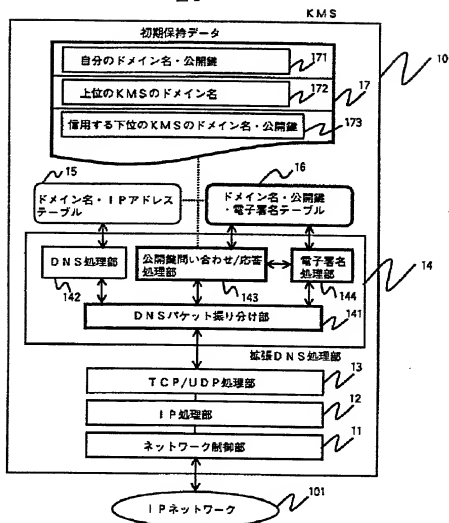


図 2

ホスト

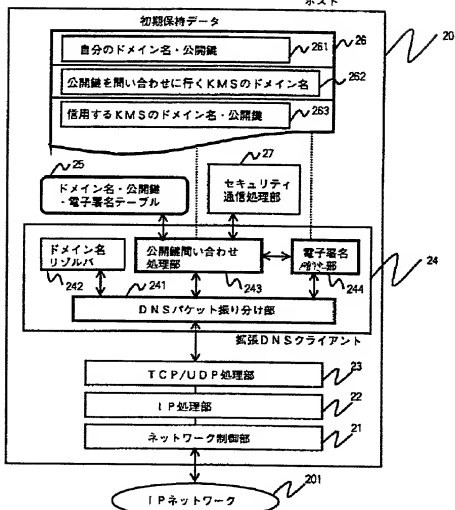


図 3

31 ドメイン名	32 公開鍵	33 電子署名	34 電子署名を付けたKMS名	35 タイムスタンプ

図 4

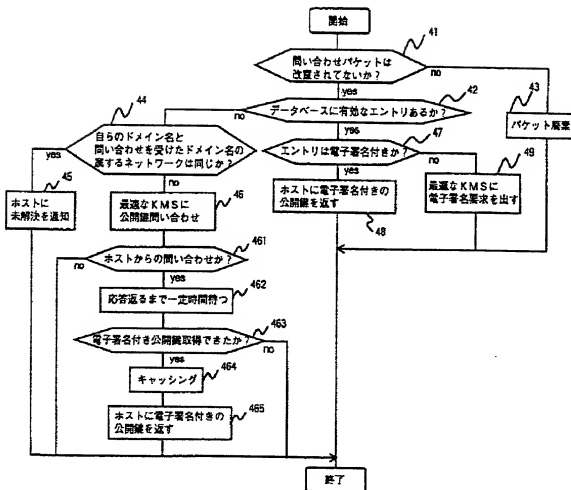


図 5

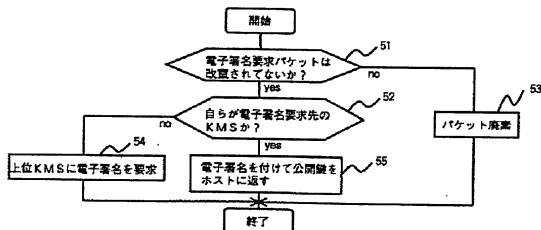
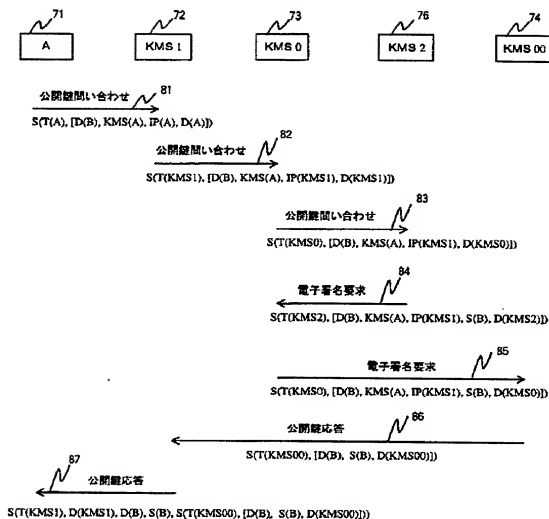


図 8



$D(X)$: Xのドメイン名
 $S(X)$: Xの公開鍵
 $T(X)$: Xの秘密鍵
 $IP(X)$: XのIPアドレス
 $KMS(X)$: Xが電子署名を要求するKMS

$S(K, [a, b, c])$: 鍵Kでメッセージ $[a, b, c]$ に電子署名をつけたもの

図 9

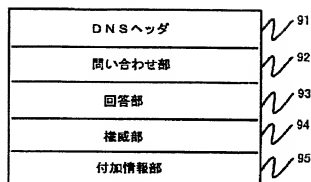
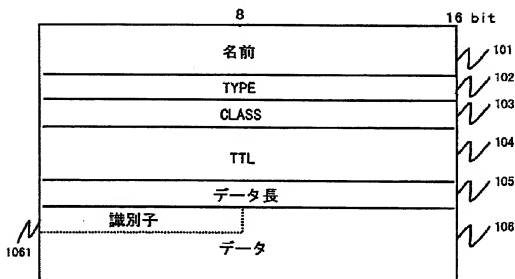


図 10



00000000000000000000000000000000